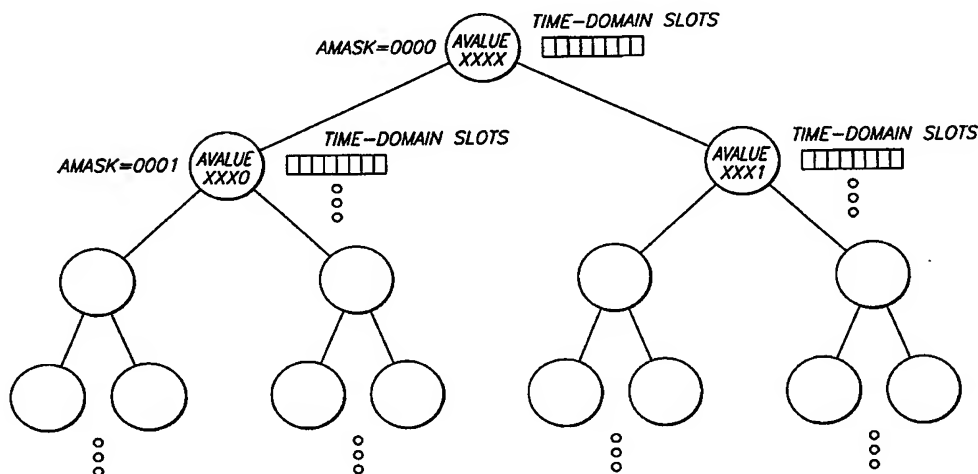




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶: H04L 12/28, G06K 7/00	A1	(11) International Publication Number: WO 99/43127 (43) International Publication Date: 26 August 1999 (26.08.99)
(21) International Application Number: PCT/US99/02288 (22) International Filing Date: 3 February 1999 (03.02.99) (30) Priority Data: 09/026,248 19 February 1998 (19.02.98) US (71) Applicant: MICRON COMMUNICATIONS, INC. [US/US]; 8000 South Federal Way, Boise, ID 83706 (US). (72) Inventors: WOOD, Clifton, W., Jr.; P.O. Box 2123, Boise, ID 83701 (US). HUSH, Don; 222 Calais, Tijeras, NM 87059 (US). (74) Agents: MALHOTRA, Deepak et al.; Wells, St. John, Roberts, Suite 1300, 601 West First Avenue, Spokane, WA 99201-3828 (US).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>

(54) Title: METHOD OF IDENTIFYING WIRELESS UNITS



(57) Abstract

A method of establishing wireless communications between an interrogator and individual ones of multiple wireless identification devices, the method comprising combining tree search and Aloha methods to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision. A system comprising an interrogator, and a plurality of wireless identification devices configured to communicate with the interrogator in a wireless fashion, the respective wireless identification devices having a unique identification number, the interrogator being configured to employ tree search and Aloha techniques to determine the unique identification numbers of the different wireless identification devices so as to be able to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision by multiple wireless identification devices attempting to respond to the interrogator at the same time.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD OF IDENTIFYING WIRELESS UNITS

5 Technical Field

This invention relates to communications protocols and to digital data communications. Still more particularly, the invention relates to data communications protocols in mediums such as radio communication or the like. The invention also relates to radio frequency identification devices for
10 inventory control, object monitoring, determining the existence, location or movement of objects, or for remote automated payment.

Background Art

Communications protocols are used in various applications. For
15 example, communications protocols can be used in electronic identification systems. As large numbers of objects are moved in inventory, product manufacturing, and merchandising operations, there is a continuous challenge to accurately monitor the location and flow of objects. Additionally, there is a continuing goal to interrogate the location of objects in an inexpensive
20 and streamlined manner. One way of tracking objects is with an electronic identification system.

One presently available electronic identification system utilizes a magnetic coupling system. In some cases, an identification device may be provided with a unique identification code in order to distinguish between a
25 number of different devices. Typically, the devices are entirely passive (have no power supply), which results in a small and portable package. However, such identification systems are only capable of operation over a relatively short range, limited by the size of a magnetic field used to supply power to the devices and to communicate with the devices.

30 Another wireless electronic identification system utilizes a large active transponder device affixed to an object to be monitored which receives a signal from an interrogator. The device receives the signal, then generates

and transmits a responsive signal. The interrogation signal and the responsive signal are typically radio-frequency (RF) signals produced by an RF transmitter circuit. Because active devices have their own power sources, and do not need to be in close proximity to an interrogator or reader to receive
5 power via magnetic coupling. Therefore, active transponder devices tend to be more suitable for applications requiring tracking of a tagged device that may not be in close proximity to an interrogator. For example, active transponder devices tend to be more suitable for inventory control or tracking.

10 Electronic identification systems can also be used for remote payment. For example, when a radio frequency identification device passes an interrogator at a toll booth, the toll booth can determine the identity of the radio frequency identification device, and thus of the owner of the device, and debit an account held by the owner for payment of toll or can receive
15 a credit card number against which the toll can be charged. Similarly, remote payment is possible for a variety of other goods or services.

A communication system, such as a wireless identification system, typically includes two transponders: a commander station or interrogator, and a responder station or transponder device which replies to the interrogator.

20 If the interrogator has prior knowledge of the identification number of a device which the interrogator is looking for, it can specify that a response is requested only from the device with that identification number. Sometimes, such information is not available. For example, there are occasions where the interrogator is attempting to determine which of multiple
25 devices are within communication range.

When the interrogator sends a message to a transponder device requesting a reply, there is a possibility that multiple transponder devices will attempt to respond simultaneously, causing a collision, and thus an erroneous message to be received by the interrogator. For example, if the interrogator
30 sends out a command requesting that all devices within a communications range identify themselves, and gets a large number of simultaneous replies,

the interrogator may not be able to interpret any of these replies. Thus, arbitration schemes are employed to permit communications free of collisions.

In one arbitration scheme or system, described in commonly assigned U.S. Patent Nos. 5,627,544; 5,583,850; 5,500,650; and 5,365,551, all to
5 Snodgrass et al. and all incorporated herein by reference, the interrogator sends a command causing each device of a potentially large number of responding devices to select a random number from a known range and use it as that device's arbitration number. By transmitting requests for identification to various subsets of the full range of arbitration numbers,
10 and checking for an error-free response, the interrogator determines the arbitration number of every responder station capable of communicating at the same time. Therefore, the interrogator is able to conduct subsequent uninterrupted communication with devices, one at a time, by addressing only one device.

15 Another arbitration scheme is referred to as the Aloha or slotted Aloha scheme. This scheme is discussed in various references relating to communications, such as Digital Communications: Fundamentals and Applications, Bernard Sklar, published January 1988 by Prentice Hall. In this type of scheme, a device will respond to an interrogator using one of many
20 time domain slots selected randomly by the device. A problem with the Aloha scheme is that if there are many devices, or potentially many devices in the field (i.e. in communications range, capable of responding) then there must be many available slots or many collisions will occur. Having many available slots slows down replies. If the magnitude of the number of devices
25 in a field is unknown, then many slots are needed. This results in the system slowing down significantly because the reply time equals the number of slots multiplied by the time period required for one reply.

An electronic identification system which can be used as a radio frequency identification device, arbitration schemes, and various applications
30 for such devices are described in detail in commonly assigned U.S. Patent Application Serial Number 08/705,043, filed August 29, 1996, and incorporated herein by reference.

Disclosure of the Invention

The invention provides a wireless identification device configured to provide a signal to identify the device in response to an interrogation signal.

One aspect of the invention provides a method of establishing wireless
5 communications between an interrogator and individual ones of multiple wireless identification devices. Tree search and Aloha methods are combined to establish communications between the interrogator and individual ones of the multiple wireless identification devices without collision.

One aspect of the invention provides a method of addressing messages
10 from an interrogator to a selected one or more of a number of communications devices. A first predetermined number of bits are established to be used as unique identification numbers. Unique identification numbers respectively having the first predetermined number of bits are established for respective devices. A second predetermined number of bits are established
15 to be used for random values. The devices are caused to select random values. Respective devices choose random values independently of random values selected by the other devices. The interrogator transmits a command requesting devices having random values within a specified group of random values to respond, the specified group being less than or equal to the entire
20 set of random values. Devices receiving the command respectively determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator within a randomly selected time slot of a number of slots. If not, they do not send a reply. The interrogator determines if a collision occurred between devices that sent a reply and, if so, creates a
25 new, smaller, specified group.

One aspect of the invention provides a communications system comprising an interrogator, and a plurality of wireless identification devices configured to communicate with the interrogator in a wireless fashion. The respective wireless identification devices have a unique identification number.
30 The interrogator is configured to employ tree search and Aloha techniques to determine the unique identification numbers of the different wireless identification devices so as to be able to establish communications between

the interrogator and individual ones of the multiple wireless identification devices without collision by multiple wireless identification devices attempting to respond to the interrogator at the same time.

Another aspect of the invention provides a system comprising an
5 interrogator configured to communicate to a selected one or more of a number of communications devices, and a plurality of communications devices. The devices are configured to select random values. Respective devices choose random values independently of random values selected by the other devices. The interrogator is configured to transmit a command requesting
10 devices having random values within a specified group of random values to respond, the specified group being less than or equal to the entire set of random values. Devices receiving the command are configured to respectively determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator within a randomly selected time slot
15 of a number of slots. If not, they do not send a reply. The interrogator is configured to determine if a collision occurred between devices that sent a reply and, if so, create a new, smaller, specified group.

One aspect of the invention provides a radio frequency identification device comprising an integrated circuit including a receiver, a transmitter, and
20 a microprocessor. In one embodiment, the integrated circuit is a monolithic single die single metal layer integrated circuit including the receiver, the transmitter, and the microprocessor. The device of this embodiment includes an active transponder, instead of a transponder which relies on magnetic coupling for power, and therefore has a much greater range.

25

Brief Description of the Drawings

Preferred embodiments of the invention are described below with reference to the following accompanying drawings.

Fig. 1 is a high level circuit schematic showing an interrogator and a
30 radio frequency identification device embodying the invention.

Fig. 2 is a front view of a housing, in the form of a badge or card, supporting the circuit of Fig. 1 according to one embodiment the invention.

Fig. 3 is a front view of a housing supporting the circuit of Fig. 1 according to another embodiment of the invention.

Fig. 4 is a diagram illustrating a tree splitting sort method for establishing communication with a radio frequency identification device in a field of a plurality of such devices, without collisions.

Fig. 5 is a time line plot illustrating operation of a slotted Aloha scheme.

Fig 6. is a diagram illustrating using a combination of a tree splitting sort method with an Aloha method for establishing communication with a radio frequency identification device in a field of a plurality of such devices.

Best Modes for Carrying Out the Invention and Disclosure of Invention

Fig. 1 illustrates a wireless identification device 12 in accordance with one embodiment of the invention. In the illustrated embodiment, the wireless identification device is a radio frequency data communication device 12, and includes RFID circuitry 16. In the illustrated embodiment, the RFID circuitry is defined by an integrated circuit as described in the above-incorporated patent application 08/705,043, filed August 29, 1996. Other embodiments are possible. A power source 18 is connected to the integrated circuit 16 to supply power to the integrated circuit 16. In one embodiment, the power source 18 comprises a battery. The device 12 further includes at least one antenna 14 connected to the circuitry 16 for wireless or radio frequency transmission and reception by the circuitry 16.

The device 12 transmits and receives radio frequency communications to and from an interrogator 26. An exemplary interrogator is described in U.S. Patent Application Serial No. 08/907,689, filed August 8, 1997 and incorporated herein by reference. Preferably, the interrogator 26 includes an antenna 28, as well as dedicated transmitting and receiving circuitry, similar to that implemented on the integrated circuit 16.

Generally, the interrogator 26 transmits an interrogation signal or command 27 via the antenna 28. The device 12 receives the incoming interrogation signal via its antenna 14. Upon receiving the signal 27, the

device 12 responds by generating and transmitting a responsive signal or reply 29. The responsive signal 29 typically includes information that uniquely identifies, or labels the particular device 12 that is transmitting, so as to identify any object or person with which the device 12 is associated.

5 Although only one device 12 is shown in Fig. 1, typically there will be multiple devices 12 that correspond with the interrogator 26, and the particular devices 12 that are in communication with the interrogator 26 will typically change over time. In the illustrated embodiment in Fig. 1, there is no communication between multiple devices 12. Instead, the devices 12
10 respectively communicate with the interrogator 26. Multiple devices 12 can be used in the same field of an interrogator 26 (i.e., within communications range of an interrogator 26). Similarly, multiple interrogators 26 can be in proximity to one or more of the devices 12.

 The radio frequency data communication device 12 can be included in
15 any appropriate housing or packaging. Various methods of manufacturing housings are described in commonly assigned U.S. Patent Application Serial No. 08/800,037, filed February 13, 1997, and incorporated herein by reference.

 Fig. 2 shows but one embodiment in the form of a card or badge 19 including the radio frequency data communication device 12, and a housing
20 11 including plastic or other suitable material. In one embodiment, the front face of the badge has visual identification features such as graphics, text, information found on identification or credit cards, etc.

 Fig. 3 illustrates but one alternative housing supporting the device 12. More particularly, Fig. 3 shows a miniature housing 20 encasing the device 12
25 to define a tag which can be supported by an object (e.g., hung from an object, affixed to an object, etc.). Although two particular types of housings have been disclosed, the device 12 can be included in any appropriate housing.

 If the power source 18 is a battery, the battery can take any suitable
30 form. Preferably, the battery type will be selected depending on weight, size, and life requirements for a particular application. In one embodiment, the battery 18 is a thin profile or button-type cell forming a small, thin energy

cell more commonly utilized in watches and small electronic devices requiring a thin profile. A conventional cell has a pair of electrodes, an anode formed by one face and a cathode formed by an opposite face. In an alternative embodiment, the power source 18 comprises a series connected pair of cells.

5 Instead of using a battery, any suitable power source can be employed.

The circuitry 16 further includes a backscatter transmitter and is configured to provide a responsive signal to the interrogator 26 by radio frequency. More particularly, the circuitry 16 includes a transmitter, a receiver, and memory such as is described in U.S. Patent Application Serial
10 Number 08/705,043.

Radio frequency identification has emerged as a viable and affordable alternative to tagging or labeling small to large quantities of items. The interrogator 26 communicates with the devices 12 via an RF link, so all transmissions by the interrogator 26 are heard simultaneously by all devices
15 12 within range.

If the interrogator 26 sends out a command requesting that all devices 12 within range identify themselves, and gets a large number of simultaneous replies, the interrogator 26 may not be able to interpret any of these replies. Therefore, arbitration schemes are provided.

20 If the interrogator 26 has prior knowledge of the identification number of a device 12 which the interrogator 26 is looking for, it can specify that a response is requested only from the device 12 with that identification number. To target a command at a specific device 12, (i.e., to initiate point-on-point communication), the interrogator 26 must send a number identifying a specific
25 device 12 along with the command. At start-up, or in a new or changing environment, these identification numbers are not known by the interrogator 26. Therefore, the interrogator 26 must identify all devices 12 in the field (within communication range) such as by determining the identification numbers of the devices 12 in the field. After this is accomplished, point-to-
30 point communication can proceed as desired by the interrogator 26.

Generally speaking, RFID systems are a type of multiaccess communication system. The distance between the interrogator 26 and devices

12 within the field is typically fairly short (e.g., several meters), so packet transmission time is determined primarily by packet size and baud rate. Propagation delays are negligible. In RFID systems, there is a potential for a large number of transmitting devices 12 and there is a need for the
5 interrogator 26 to work in a changing environment, where different devices 12 are swapped in and out frequently (e.g., as inventory is added or removed). The inventors have determined that, in such systems, the use of random access methods work effectively for contention resolution (i.e., for dealing with collisions between devices 12 attempting to respond to the
10 interrogator 26 at the same time).

RFID systems have some characteristics that are different from other communications systems. For example, one characteristic of the illustrated RFID systems is that the devices 12 never communicate without being prompted by the interrogator 26. This is in contrast to typical multiaccess
15 systems where the transmitting units operate more independently. In addition, contention for the communication medium is short lived as compared to the ongoing nature of the problem in other multiaccess systems. For example, in a RFID system, after the devices 12 have been identified, the interrogator can communicate with them in a point-to-point fashion.
20 Thus, arbitration in a RFID system is a transient rather than steady-state phenomenon. Further, the capability of a device 12 is limited by practical restrictions on size, power, and cost. The lifetime of a device 12 can often be measured in terms of number of transmissions before battery power is lost. Therefore, one of the most important measures of system performance in
25 RFID arbitration is total time required to arbitrate a set of devices 12. Another measure is power consumed by the devices 12 during the process. This is in contrast to the measures of throughput and packet delay in other types of multiaccess systems.

Fig. 4 illustrates one arbitration scheme that can be employed for
30 communication between the interrogator and devices 12. Although the arbitration system is being described in connection with a wireless identification system or RFID system, this and other arbitration schemes

disclosed herein can be employed in any communication system. Generally, the interrogator 26 sends a command causing each device 12 of a potentially large number of responding devices 12 to select a random number from a known range and use it as that device's arbitration number. By transmitting
5 requests for identification to various subsets of the full range of arbitration numbers, and checking for an error-free response, the interrogator 26 determines the arbitration number of every responder station capable of communicating at the same time. Therefore, the interrogator 26 is able to conduct subsequent uninterrupted communication with devices 12, one at a
10 time, by addressing only one device 12.

Three variables are used: an arbitration value (AVALUE), an arbitration mask (AMASK), and a random value ID (RV). The interrogator sends a command causing each device of a potentially large number of responding devices to select a random number from a known
15 range and use it as that device's arbitration number. The interrogator sends an arbitration value (AVALUE) and an arbitration mask (AMASK) to a set of devices 12. The receiving devices 12 evaluate the following equation: $(AMASK \& AVALUE) == (AMASK \& RV)$ wherein "&" is a bitwise AND function, and wherein "==" is an equality function. If the equation
20 evaluates to "1" (TRUE), then the device 12 will reply. If the equation evaluates to "0" (FALSE), then the device 12 will not reply. By performing this in a structured manner, with the number of bits in the arbitration mask being increased by one each time, eventually a device 12 will respond with no collisions. Thus, a binary search tree methodology is employed.

25 An example using actual numbers will now be provided using only four bits, for simplicity, reference being made to Fig. 4. In one embodiment, sixteen bits are used for AVALUE and AMASK, respectively. Other numbers of bits can also be employed depending, for example, on the number of devices 12 expected to be encountered in a particular application, on
30 desired cost points, etc.

Assume, for this example, that there are two devices 12 in the field, one with a random value (RV) of 1100 (binary), and another with a random

value (RV) of 1010 (binary). The interrogator is trying to establish communications without collisions being caused by the two devices 12 attempting to communicate at the same time.

The interrogator sets AVALUE to 0000 (or all "don't care", indicated
5 by the character "X" in Fig. 4) and AMASK to 0000. The interrogator transmits a command to all devices 12 requesting that they identify themselves. Each of the devices 12 evaluate $(AMASK \& AVALUE) == (AMASK \& RV)$ using the random value RV that the respective devices 12 selected. If the equation evaluates to "1" (TRUE),
10 then the device 12 will reply. If the equation evaluates to "0" (FALSE), then the device 12 will not reply. In the first level of the illustrated tree, AMASK is 0000 and anything bitwise ANDed with all zeros results in all zeros, so both the devices 12 in the field respond, and there is a collision.

Next, the interrogator sets AMASK to 0001 and AVALUE to 0000 and
15 transmits an identify command. Both devices 12 in the field have a zero for their least significant bit, and $(AMASK \& AVALUE) == (AMASK \& RV)$ will be true for both devices 12. For the device 12 with a random value of 1100, the left side of the equation is evaluated as follows $(0001 \& 0000) = 0000$. The right side is evaluated as $(0001 \& 1100) = 0000$. The left
20 side equals the right side, so the equation is true for the device 12 with the random value of 1100. For the device 12 with a random value of 1010, the left side of the equation is evaluated as $(0001 \& 0000) = 0000$. The right side is evaluated as $(0001 \& 1010) = 0000$. The left side equals the right side, so the equation is true for the device 12 with the random value of 1010.
25 Because the equation is true for both devices 12 in the field, both devices 12 in the field respond, and there is another collision.

Recursively, the interrogator next sets AMASK to 0011 with AVALUE still at 0000 and transmits an identify command. $(AMASK \& AVALUE) == (AMASK \& RV)$ is evaluated for both devices 12.
30 For the device 12 with a random value of 1100, the left side of the equation is evaluated as follows $(0011 \& 0000) = 0000$. The right side is evaluated as $(0011 \& 1100) = 0000$. The left side equals the right side, so the equation is

true for the device 12 with the random value of 1100, so this device 12 responds. For the device 12 with a random value of 1010, the left side of the equation is evaluated as $(0011 \& 0000)=0000$. The right side is evaluated as $(0011 \& 1010)=0010$. The left side does not equal the right
5 side, so the equation is false for the device 12 with the random value of 1010, and this device 12 does not respond. Therefore, there is no collision, and the interrogator can determine the identity (e.g., an identification number) for the device 12 that does respond.

De-recursion takes place, and the devices 12 to the right for the same
10 AMASK level are accessed by setting AVALUE at 0010 and using the same AMASK value 0011.

The device 12 with the random value of 1010 receives a command and evaluates the equation $(AMASK \& AVALUE)=(AMASK \& RV)$. The left side of the equation is evaluated as $(0011 \& 0010)=0010$. The right side of
15 the equation is evaluated as $(0011 \& 1010)=0010$. The right side equals the left side, so the equation is true for the device 12 with the random value of 1010. Because there are no other devices 12 in the subtree, a good reply is returned by the device 12 with the random value of 1010. There is no collision, and the interrogator can determine the identity (e.g., an
20 identification number) for the device 12 that does respond.

By recursion, what is meant is that a function makes a call to itself. In other words, the function calls itself within the body of the function. After the called function returns, de-recursion takes place and execution continues at the place just after the function call; i.e. at the beginning of the
25 statement after the function call.

For instance, consider a function that has four statements (numbered 1,2,3,4) in it, and the second statement is a recursive call. Assume that the fourth statement is a return statement. The first time through the loop (iteration 1) the function executes the statement 2 and (because it is a
30 recursive call) calls itself causing iteration 2 to occur. When iteration 2 gets to statement 2, it calls itself making iteration 3. During execution in iteration 3 of statement 1, assume that the function does a return. The

information that was saved on the stack from iteration 2 is loaded and the function resumes execution at statement 3 (in iteration 2), followed by the execution of statement 4 which is also a return statement. Since there are no more statements in the function, the function de-recurses to iteration 1.

5 Iteration 1, had previously recursively called itself in statement 2. Therefore, it now executes statement 3 (in iteration 1). Following that it executes a return at statement 4. Recursion is known in the art.

Consider the following code, which employs recursion, and which can be used to implement operation of the method shown in Fig. 4 and described
10 above.

```

Arbitrate(AMASK, AVALUE)
{
    collision=IdentifyCmnd(AMASK, AVALUE)
15    if (collision) then
        {
            /* recursive call for left side */
            Arbitrate((AMASK<<1)+1, AVALUE)
            /* recursive call for right side */
20            Arbitrate((AMASK<<1)+1, AVALUE+(AMASK+1))
        } /* endif */
    } /* return */

```

25 The symbol "<<" represents a bitwise left shift. "<<1" means shift left by one place. Thus, 0001 << 1 would be 0010. Note, however, that AMASK is originally called with a value of zero, and 0000 << 1 is still 0000. Therefore, for the first recursive call, AMASK = (AMASK << 1)+1.
30 So for the first recursive call, the value of AMASK is 0000+0001=0001. For the second call, AMASK=(0001 << 1)+1=0010+1=0011. For the third recursive call, AMASK=(0011 << 1)+1=0110+1=0111.

The routine generates values for AMASK and AVALUE to be used by the interrogator in an identify command "IdentifyCmnd." Note that the
35 routine calls itself if there is a collision. De-recursion occurs when there is no collision. AVALUE and AMASK would have values such as the following assuming there are collisions all the way down to the bottom of the tree.

	AVALUE	AMASK
	0000	0000
	0000	0001
	0000	0011
5	0000	0111
	0000	1111*
	1000	1111*
	0100	0111
	0100	1111*
10	1100	1111*

This sequence of AMASK, AVALUE binary numbers assumes that there are collisions all the way down to the bottom of the tree, at which point the Identify command sent by the interrogator is finally successful so that no collision occurs. Rows in the table for which the interrogator is successful in receiving a reply without collision are marked with the symbol “*”. Note that if the Identify command was successful at, for example, the third line in the table then the interrogator would stop going down that branch of the tree and start down another, so the sequence would be as shown in the following table.

	AVALUE	AMASK
	0000	0000
	0000	0001
25	0000	0011*
	0010	0011

This method is referred to as a splitting method. It works by splitting groups of colliding devices into subsets that are resolved in turn. The splitting method can also be viewed as a type of tree search. Each split

moves the method one level deeper in the tree. Either depth-first or breadth first traversals of the tree can be employed.

Another arbitration method that can be employed is referred to as the "Aloha" method. In the Aloha method, every time a device 12 is involved
5 in a collision, it waits a random period of time before retransmitting. This method can be improved by dividing time into equally sized slots and forcing transmissions to be aligned with one of these slots. This is referred to as "slotted Aloha." In operation, the interrogator asks all devices 12 in the field to transmit their identification numbers in the next time slot. If the
10 response is garbled, the interrogator informs the devices 12 that a collision has occurred, and the slotted Aloha scheme is put into action. This means that each device 12 in the field responds within an arbitrary slot determined by a randomly selected value. In other words, in each successive time slot, the devices 12 decide to transmit their identification number with a certain
15 probability.

The Aloha method is based on a system operated by the University of Hawaii. In 1971, the University of Hawaii began operation of a system named Aloha. A communication satellite was used to interconnect several university computers by use of a random access protocol. The system
20 operates as follows. Users or devices transmit at any time they desire. After transmitting, a user listens for an acknowledgment from the receiver or interrogator. Transmissions from different users will sometimes overlap in time (collide), causing reception errors in the data in each of the contending messages. The errors are detected by the receiver, and the receiver sends a
25 negative acknowledgment to the users. When a negative acknowledgment is received, the messages are retransmitted by the colliding users after a random delay. If the colliding users attempted to retransmit without the random delay, they would collide again. If the user does not receive either an acknowledgment or a negative acknowledgment within a certain amount of
30 time, the user "times out" and retransmits the message.

In the slotted Aloha scheme, a sequence of coordination pulses is broadcast to all stations (devices). As is the case with the pure Aloha

scheme, packet lengths are constant. Messages are required to be sent in a slot time between synchronization pulses, and can be started only at the beginning of a time slot. This reduces the rate of collisions because only messages transmitted in the same slot can interfere with one another. The
5 retransmission mode of the pure Aloha scheme is modified for slotted Aloha such that if a negative acknowledgment occurs, the device retransmits after a random delay of an integer number of slot times.

Fig. 5 illustrates operation of the slotted Aloha scheme. Fig. 5 shows a packet of data bits transmitted by a first device 12a, which is substantially
10 identical to the device 12. The interrogator 26 acknowledges receipt without collision, as indicated in Fig. 5 by the symbol ACK. Fig. 5 also shows devices 12b and 12c, also substantially identical to the device 12, simultaneously transmitting packets of data to the interrogator 26, resulting in a collision. The interrogator returns a negative acknowledgment, as
15 indicated in Fig. 5 by the symbol NAK. The devices 12b and 12c then respectively select random numbers, and retransmit after a time delay corresponding to the selected random number. There is a possibility that the devices 12b and 12c will again transmit at the same times, causing another collision, but in that case they will retransmit again using newly selected
20 random numbers until there is no collision.

Another form of Aloha scheme is called reservation-Aloha. The reservation-Aloha system has two basic modes: an unreserved mode, and a reserved mode.

In the unreserved mode, a time frame is established and divided into
25 a number of small reservation subslots. Users (devices) use these subslots to reserve message slots. After requesting a reservation, the user (device) listens for an acknowledgment and a slot assignment.

In the reserved mode, a time frame is divided into a certain number of slots whenever a reservation is made. All but the last slot are used for
30 message transmissions. The last slot is subdivided into subslots to be used for reservations. Users (devices) send message packets in their assigned portions of the slots reserved for message transmissions.

Fig. 6 illustrates combining a tree sort method of a type such as the one shown in Fig. 4 with an Aloha method. Combining the two methods allows a minimal number of slots to be used and takes advantage of the conquer and divide approach of the tree sort method. The method shown
5 in Fig. 6 proceeds in a manner similar to the manner described in connection with Fig. 4, except that devices 12 in the field that reply for the given AMASK and AVALUE, reply within a randomly selected time slot. This significantly reduces the number of collisions. In one embodiment, the reply includes the unique identification number of the particular device 12. In one
10 embodiment, the reply includes the random value RV selected by the particular device 12. In one embodiment, the reply includes both the unique identification number of the particular device 12 as well as the random value RV selected by the same device 12.

In one embodiment, the same randomly selected time slot is used by
15 a device 12 at different levels of the tree (i.e., for different values of AMASK and AVALUE). In another embodiment, different randomly selected times slots are used by a device 12 at different levels of the tree (i.e., for different values of AMASK and AVALUE). In one embodiment, a combination of these approaches is used. For example, one embodiment
20 utilizes a method where the interrogator goes down the tree until some responses without collision are received, before the devices 12 re-randomize their Aloha random number. This can be classified as an adaptive method. Other adaptive methods are possible. For example, in one embodiment, the number of Aloha slots is reduced at lower levels of the tree. The number
25 of slots can be reduced by the same number for each level down the tree, or by a number that varies depending on the number of levels down the tree. Thus, for example, the number of slots can remain constant through a progression down the tree until some responses without collision are received, at which point the number of slots is reduced.

30 Thus, this embodiment provides the advantages of both the Aloha methods and the tree sorting methods of establishing communications without collisions.

In another embodiment, levels of the search tree are skipped. Skipping levels in the tree, after a collision caused by multiple devices 12 responding, reduces the number of subsequent collisions without adding significantly to the number of no replies. In real-time systems, it is desirable
5 to have quick arbitration sessions on a set of devices 12 whose unique identification numbers are unknown. Level skipping reduces the number of collisions, both reducing arbitration time and conserving battery life on a set of devices 12. In one embodiment, every other level is skipped. In alternative embodiments, more than one level is skipped each time.

10 The trade off that must be considered in determining how many (if any) levels to skip with each descent down the tree is as follows. Skipping levels reduces the number of collisions, thus saving battery power in the devices 12. Skipping deeper (skipping more than one level) further reduces the number of collisions. The more levels that are skipped, the greater the
15 reduction in collisions. However, skipping levels results in longer search times because the number of queries (Identify commands) increases. The more levels that are skipped, the longer the search times. Skipping just one level has an almost negligible effect on search time, but drastically reduces the number of collisions. If more than one level is skipped, search time
20 increases substantially. Skipping every other level drastically reduces the number of collisions and saves battery power without significantly increasing the number of queries.

Level skipping methods are described in a commonly assigned patent application (attorney docket MI40-117) naming Clifton W. Wood, Jr. and Don
25 Hush as inventors, titled "Method of Addressing Messages, Method of Establishing Wireless Communications, and Communications System," filed concurrently herewith, and incorporated herein by reference.

CLAIMS

1. A method of establishing wireless communications between an interrogator and individual multiple wireless identification devices, the method comprising combining tree search and Aloha methods to establish
5 communications between the interrogator and individual of multiple wireless identification devices.

2. A method in accordance with claim 1 wherein the combined Aloha methods are slotted Aloha methods.

10

3. A method in accordance with claim 1 wherein the wireless identification device comprises an integrated circuit including a receiver, a modulator, and a microprocessor in communication with the receiver and modulator.

15

4. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices, the method comprising:

establishing a first predetermined number of bits to be used as unique
20 identification numbers, and establishing for respective devices unique identification numbers respectively having the first predetermined number of bits;

establishing a second predetermined number of bits to be used for random values;

25 causing the devices to select random values, wherein respective devices choose random values independently of random values selected by the other devices;

transmitting a command from the interrogator requesting devices having random values within a specified group of random values to respond, the
30 specified group being less than or equal to the entire set of random values;

receiving the command at multiple devices, the devices receiving the command respectively determining if the random value chosen by the

command falls within the specified group and, if so, sending a reply to the interrogator within a randomly selected time slot of a number of slots; and, if not, not sending a reply; and

determining with the interrogator if a collision occurred between
5 devices that sent a reply and, if so, creating a new, smaller, specified group.

5. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein the sending of a reply to the interrogator within a
10 randomly selected time slot is in accordance with an Aloha method.

6. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein the sending of a reply to the interrogator within a
15 randomly selected time slot is in accordance with a slotted Aloha method.

7. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein the method is an adaptive method.

20

8. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein the number of slots is four.

25 9. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein sending a reply to the interrogator comprises transmitting the unique identification number of the device sending the reply.

30

10. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein sending a reply to the interrogator comprises transmitting the random value of the device sending the reply.

5

11. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein, after receiving a reply without collision from a device, the interrogator sends a command individually addressed to that device.

10

12. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 4 wherein the time slot randomly selected by a device is selected using a random number different from the random value of that device.

15

13. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices, the method comprising:

establishing unique identification numbers for respective devices;

20 causing the devices to select random values, wherein respective devices choose random values independently of random values selected by the other devices;

transmitting from the interrogator a command requesting devices having random values within a specified group of random values to respond, the
25 specified group being less than or equal to the entire set of random values;

receiving the command at multiple devices, the devices receiving the command respectively determining if the random value chosen by the device falls within the specified group and, if so, sending a reply to the interrogator within a randomly selected time slot of a number of slots; and, if not, not
30 sending a reply; and

determining using the interrogator if a collision occurred between devices that sent a reply and, if so, creating a new, smaller, specified group.

14. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 13 wherein establishing unique identification numbers for respective devices comprises establishing a predetermined number of bits to
5 be used for the unique identification numbers.

15. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 14 and further including establishing a predetermined number of
10 bits to be used for the random values.

16. A method of addressing messages from an interrogator to a selected one or more of a number of communications devices in accordance with claim 15 wherein the predetermined number of bits to be used for the
15 random values comprises sixteen bits.

17. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices, the method comprising:
establishing for respective devices unique identification numbers
20 respectively having a first predetermined number of bits;

establishing a second predetermined number of bits to be used for random values;

causing the devices to select random values, wherein respective devices choose random values independently of random values selected by the other
25 devices;

transmitting from the interrogator a command requesting devices having random values within a specified group of random values to respond, the specified group being less than or equal to the entire set of random values;

receiving the command at multiple devices, the devices receiving the
30 command respectively determining if the random values chosen by the device falls within the specified group and, if so, sending a reply to the interrogator within a randomly selected time slot of a number of possible time slots, in

accordance with an Aloha method; and, if not, not sending a reply, wherein sending a reply to the interrogator comprises transmitting both the random value of the device sending the reply and the unique identification number of the device sending the reply, and wherein the time slot randomly selected
5 by a device is selected using a random number different from the random value of that device;

determining with the interrogator if a collision occurred between devices that sent a reply and, if so, creating a new, smaller, specified group; and

10 if a reply without collision is received from a device, the interrogator subsequently sending a command individually addressed to that device.

18. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim
15 17 wherein the number of possible time slots is four.

19. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim 17 wherein the number of possible time slots is four, wherein the first
20 predetermined number of bits is sixteen, and wherein the second predetermined number of bits is sixteen.

20. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim
25 17 wherein the number of possible slots varies from one specified group to another.

21. A method of addressing messages from an interrogator to a selected one or more of a number of RFID devices in accordance with claim
30 17 and further comprising, after creating a new, smaller, specified group:

the interrogator transmitting a command requesting devices having random values within a specified group of random values to respond, the

specified group being less than or equal to the entire set of random values;
and

devices receiving the command respectively determining if their chosen
random values fall within the new smaller specified group and, if so, sending
5 a reply to the interrogator within a randomly selected time slot of a number
of possible time slots, in accordance with an Aloha method.

22. A method of addressing messages from an interrogator to a
selected one or more of a number of RFID devices in accordance with claim
10 21 and further comprising the subsequent steps of the interrogator
determining if a collision occurred between devices that sent a reply and, if
so, creating a new specified group and repeating the transmitting of the
command requesting devices having random values within a specified group
of random values to respond using different specified groups until all devices
15 are identified, for every command the devices receiving the command
determining if their chosen random values fall within the specified group and,
if so, sending a reply to the interrogator within a randomly selected time slot
of a number of possible time slots, in accordance with an Aloha method.

20 23. A communications system comprising an interrogator, and a
plurality of wireless identification devices configured to communicate with the
interrogator in a wireless fashion, the respective wireless identification devices
having a unique identification number, the interrogator being configured to
employ tree search and Aloha techniques to determine the unique
25 identification numbers of the different wireless identification devices so as to
be able to establish communications between the interrogator and individual
ones of the multiple wireless identification devices without collision by
multiple wireless identification devices attempting to respond to the
interrogator at the same time.

30

24. A communications system in accordance with claim 23 wherein
the Aloha technique is a slotted Aloha technique.

25. A communications system in accordance with claim 23 wherein the wireless identification device comprises an integrated circuit including a receiver, a modulator, and a microprocessor in communication with the receiver and modulator.

5

26. A system comprising:

an interrogator;

a number of communications devices capable of wireless communications with the interrogator;

10 means for establishing a first predetermined number of bits to be used as unique identification numbers, and for establishing for respective devices unique identification numbers respectively having the first predetermined number of bits;

means for establishing a second predetermined number of bits to be
15 used for random values;

means for causing the devices to select random values, wherein respective devices choose random values independently of random values selected by the other devices;

means for causing the interrogator to transmit a command requesting
20 devices having random values within a specified group of random values to respond, the specified group being less than or equal to the entire set of random values;

means for causing devices receiving the command to determine if their chosen random values fall within the specified group and, if so, send a reply
25 to the interrogator within a randomly selected time slot of a number of slots; and, if not, not send a reply; and

means for causing the interrogator to determine if a collision occurred between devices that sent a reply and, if so, create a new, smaller, specified group.

30

27. A system in accordance with claim 26 wherein the sending of a reply to the interrogator within a randomly selected time slot is in accordance with an Aloha technique.

5 28. A system in accordance with claim 26 wherein the sending of a reply to the interrogator within a randomly selected time slot is in accordance with a slotted Aloha technique.

29. A system in accordance with claim 26 wherein the number of
10 slots is four.

30. A system in accordance with claim 26 wherein sending a reply to the interrogator comprises transmitting the unique identification number of the device sending the reply.

15

31. A system in accordance with claim 26 wherein sending a reply to the interrogator comprises transmitting the random value of the device sending the reply.

20 32. A system in accordance with claim 26 wherein sending a reply to the interrogator comprises transmitting both the random value of the device sending the reply and the unique identification number of the device sending the reply.

25 33. A system in accordance with claim 26 wherein the interrogator further includes means for, after receiving a reply without collision from a device, sending a command individually addressed to that device.

34. A system in accordance with claim 26 wherein the time slot
30 randomly selected by a device is selected using a random number different from the random value of that device.

35. A system comprising:

an interrogator configured to communicate to a selected one or more of a number of communications devices;

a plurality of communications devices;

5 the devices being configured to select random values, wherein respective devices choose random values independently of random values selected by the other devices;

the interrogator being configured to transmit a command requesting devices having random values within a specified group of random values to
10 respond, the specified group being less than or equal to the entire set of random values;

devices receiving the command being configured to respectively determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator within a randomly selected time slot
15 of a number of slots; and, if not, not send a reply; and

the interrogator being configured to determine if a collision occurred between devices that sent a reply and, if so, create a new, smaller, specified group.

20 36. A system in accordance with claim 35 wherein the predetermined number of bits to be used for the random values comprises sixteen bits.

37. A system comprising:

an interrogator configured to communicate to a selected one or more
25 of a number of communications devices;

a plurality of communications devices, respective devices being configured to store unique identification numbers respectively having a first predetermined number of bits, respective devices being further configured to store a second predetermined number of bits to be used for random values,
30 respective devices being configured to select random values independently of random values selected by the other devices;

the interrogator being configured to transmit a command requesting devices having random values within a specified group of random values to respond, the specified group being less than or equal to the entire set of random values;

5 devices receiving the command respectively being configured to determine if their chosen random values fall within the specified group and, if so, send a reply to the interrogator within a randomly selected time slot of a number of possible time slots, in accordance with an Aloha technique; and, if not, not send a reply, wherein sending a reply to the interrogator
10 comprises transmitting both the random value of the device sending the reply and the unique identification number of the device sending the reply, and wherein the time slot randomly selected by a device is selected using a random number different from the random value of that device;

the interrogator being configured to determine if a collision occurred
15 between devices that sent a reply and, if so, create a new, smaller, specified group; and

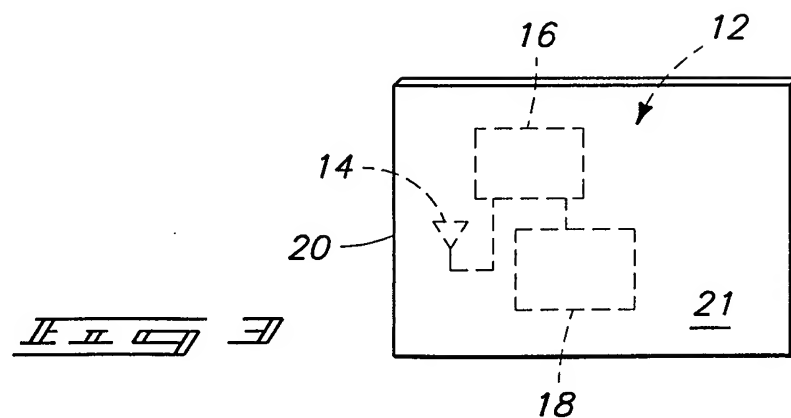
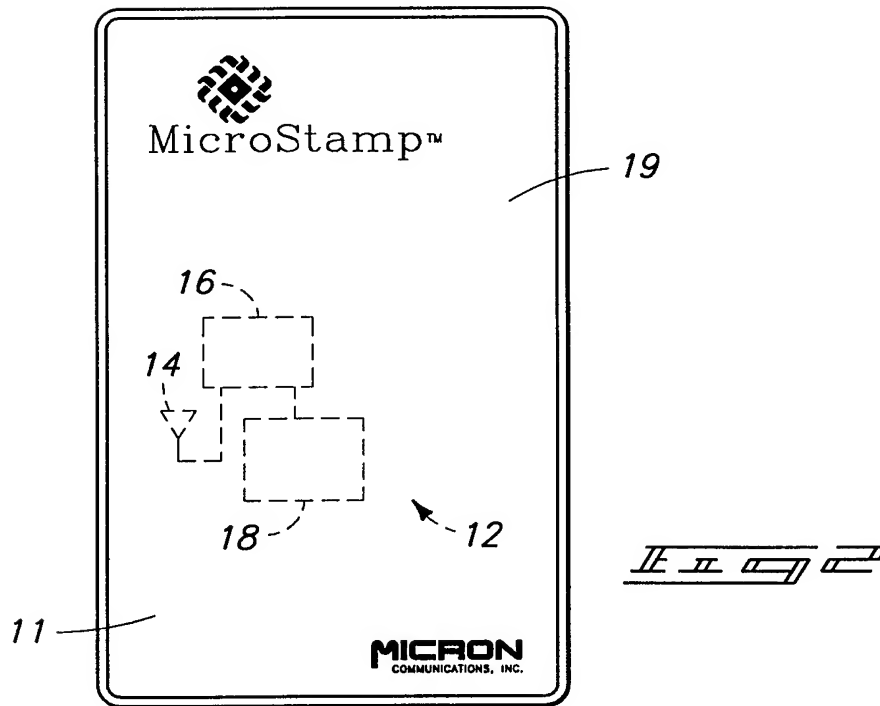
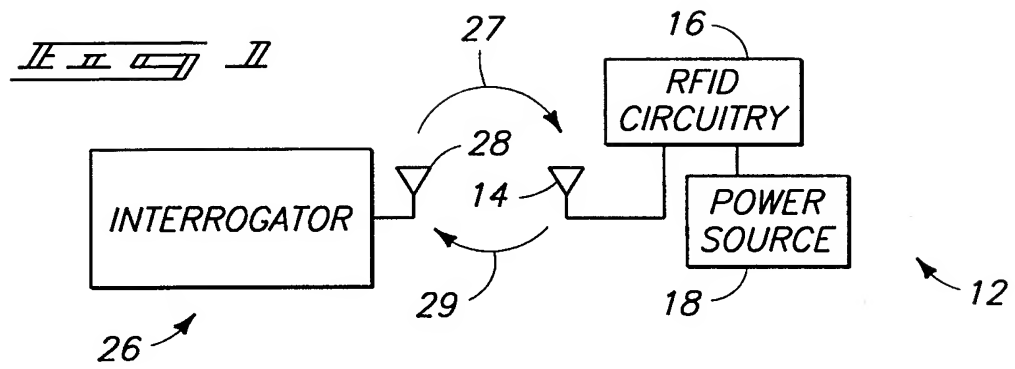
the interrogator being configured to send a command individually addressed to a device after communicating with a device without a collision.

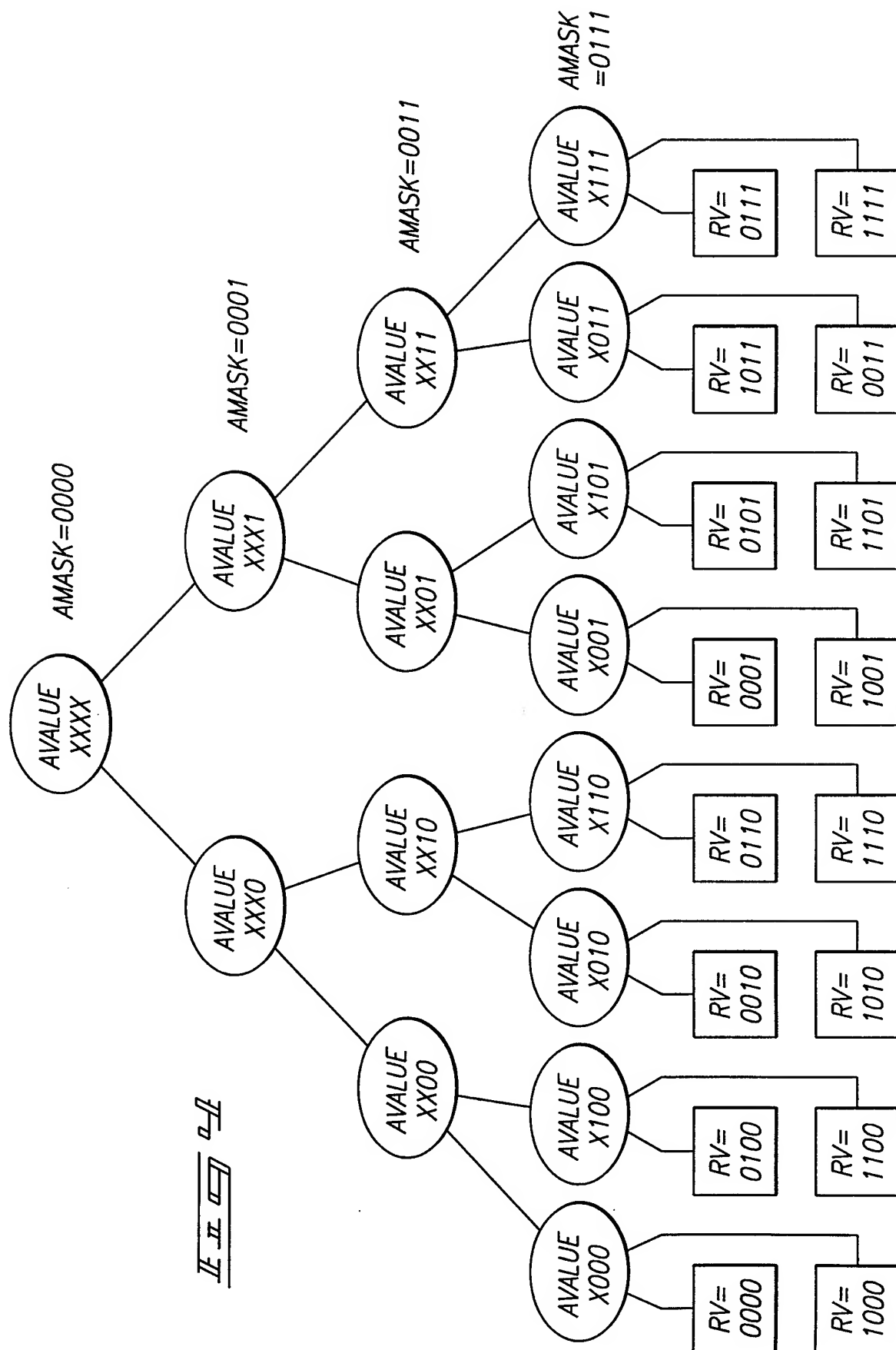
20 38. A system in accordance with claim 37 wherein the number of possible time slots is four.

39. A system in accordance with claim 37 wherein the number of possible time slots is four, wherein the first predetermined number of bits is
25 sixteen, and wherein the second predetermined number of bits is sixteen.

40. A system in accordance with claim 37 wherein the number of possible slots varies from one specified group to another.

1/4





3/4

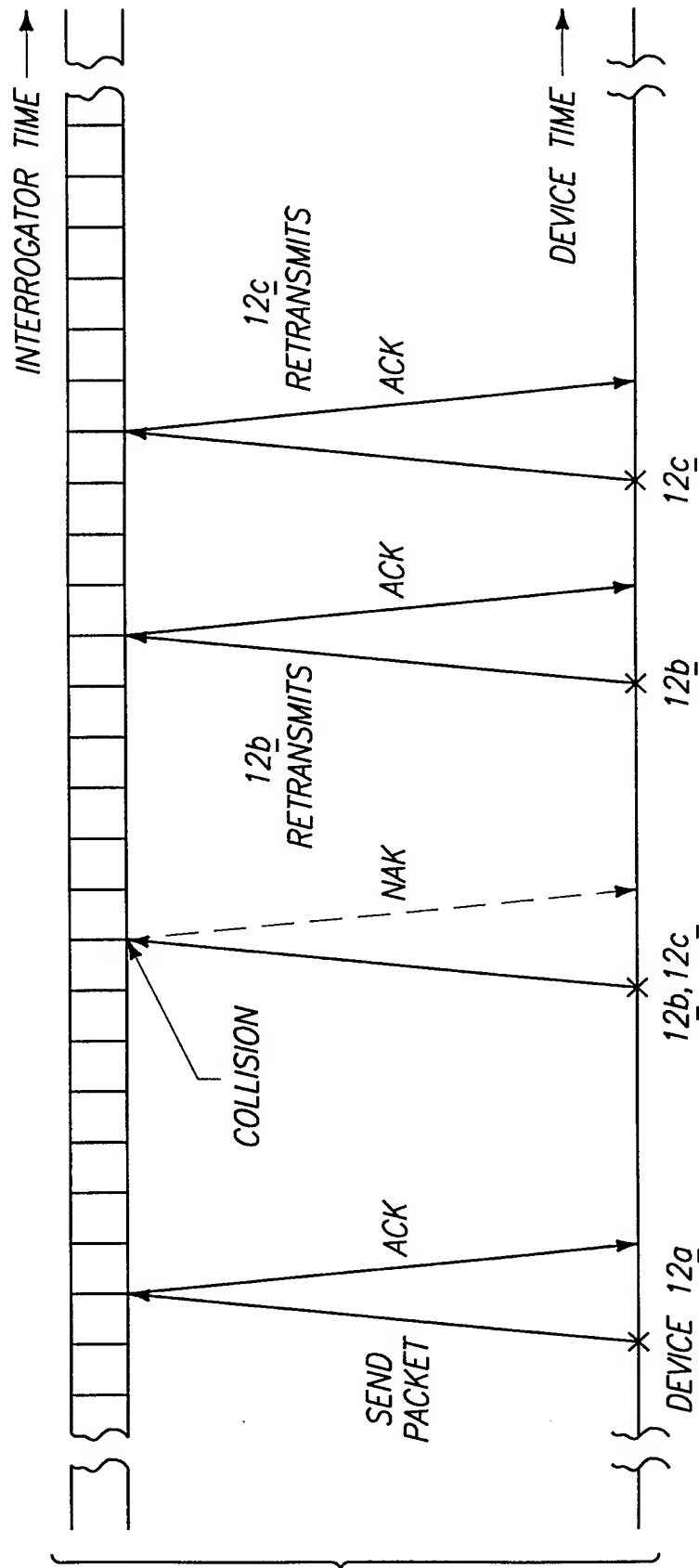
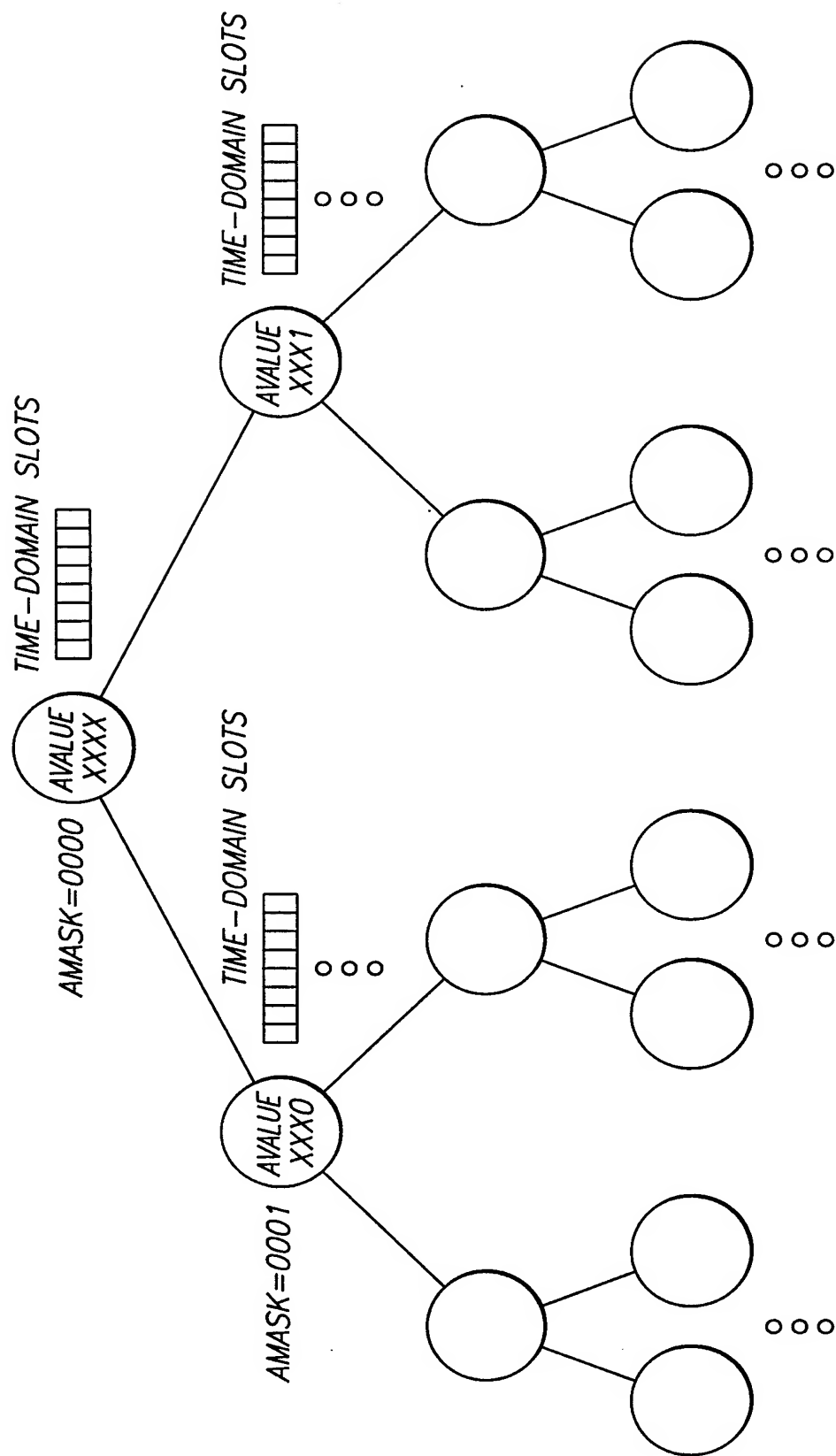


FIG. 3

4/4



11 11 11 11

INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 99/02288

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/28 G06K7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 365 551 A (SNODGRASS CHARLES K ET AL) 15 November 1994 (1994-11-15) cited in the application column 9, line 61 - column 11, line 68 column 13, line 67 - column 15, line 35 column 17, line 7 - column 19, line 63 figure 12	1,23
Y		2-22, 24-40
Y	EP 0 779 520 A (AT & T CORP) 18 June 1997 (1997-06-18) column 6, line 6 - line 48 figure 9	2-22, 24-40

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

21 July 1999

Date of mailing of the international search report

03/08/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Ströbeck, A

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 99/02288

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5365551 A	15-11-1994	US 5583850 A	10-12-1996
		US 5787174 A	28-07-1998
		US 5841770 A	24-11-1998
EP 0779520 A	18-06-1997	CA 2190546 A	13-06-1997
		JP 9238115 A	09-09-1997